REMARKS

The applicant appreciates the careful examination the Examiner has given to this application and believes the claims as amended satisfy the Examiner's concerns.

With regard to Section 7 of the Action, the Examiner has rejected Claim 19 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement, wherein the specification does not clearly define network resource management.

Paragraph [0056] in the written description of the present invention describes the resources used during the session as being (session duration, data transferred, etc.) and the SNMP management for managing these resources. Hence, the SNMP is being defined in the specification for network resource management.

It is respectfully submitted that this rejection of the Examiner has been traversed.

With regard to Section 9 of the Action, the Examiner has rejected claims 21-22 & 24 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 21-22 & 24 have been amended to further clarify the invention and to overcome the rejection of the Examiner.

With regard to Section 11 of the Action, the Examiner has rejected claims 1-4, 6-7, 11-12, 15, 17, 20 & 25 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,463,474 to Fuh et al. (Fuh).

Claim 1 has been amended by introducing additional limitations to better define the invention and to further differentiate from the cited prior art references.

Claim 1 as amended provides a distributed subscriber management (DSM) method for controlling user authentication at an access control node located between plurality of user networks and plurality of ISP (Internet service Provider) networks via an access network. The DSM method comprises receiving, at the access control node, which is operatively connected to the plurality of user networks, a data unit from a user located on one of the plurality of user networks for accessing at least one of the plurality of ISP networks connected to the access network; and determining whether the data unit requires authentication for accessing the at least one of the

plurality of ISP networks. If the data unit requires authentication, determining whether authentication data for the at least one of the plurality of ISP networks is locally stored in a local authorization table on the access control node. The local authorization table comprises the authenticated data unit for the plurality of ISP networks.

Advantageously, the method in the amended claim 1 provides the ability of a user network to select from a number of ISPs (Internet service providers) and connect to the selected ISP network. Multiple ISP selection has not traditionally been regarded as an ability of networks but is now seen as a necessary feature for products providing access network services. In the present invention the user has the capability of switching between destination ISPs or corporations via the DSM method.

Further, if the authentication data is locally stored in the local authorization table on the access control node, authenticating the data unit, thus preventing unnecessary traffic interchange between the access network, the plurality of ISP networks, and the plurality of user networks. If the authentication data is not locally stored in the local authorization table on the access control node, determining whether the data unit is eligible for transmission to the at least one of the plurality of ISP networks ; and if the data unit is eligible for transmission, transmitting the data unit from the access control node to the at least one of the plurality of ISP networks .

Appreciatively, the method in the amended claim 1 provides the ability for user networks and users to connect to numerous supported ISP networks and services.

In contrast, (Fuh) teaches a method for an access control device, which is designed for communication with a single external (or specific) network. Fig.4 & Fig. 7A, # 702 in (Fuh) illustrate the access control device communicating with a single external network. The communications between the user network, access control device, and this single external network are shown in Fig. 7A, #702, # 704, and #706. In Fig. 7A, #708, the searching is performed for the authenticated data for users wishing to connect to this single external network (i.e., in terms of IP address) and the interrogation of the users, (Fig. 7B, 724 & Fig. 5A), are for users access to a single external network. In (Fuh), col. 12, lines 43-44, Fig. 7B, #730, 732, 736, 740, and col.11, lines 46-48, teach the well known process for authenticating the data unit for a user to permit the user to access this single specific external network.

Claims 2-3 depend on the amended claim 1 and have been amended by introducing additional limitations to better define the invention.

Claim 4 has been canceled without prejudice.

Claim 6 depends on the amended claim 1 and has been amended by introducing additional limitations to better define the invention.

Claims 7, and 11-12 depend on the amended claim 1.

Claim 15 is a system claim and has similar scope as the amended claim 1 and has been amended by introducing additional limitations to better define the invention and to further differentiate from the cited prior art references.

Claims 17, 20, and 25 depend on the amended claim 15 and have been amended by introducing additional limitations to better define the invention.

It is respectfully submitted that the anticipation rejection of the Examiner in view of (Fuh) has been traversed.

With regard to Section 13 of the Action, the Examiner has rejected claim 5 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 2 above, in further view of U.S. Patent 5,491,752 to Kaufman et al. (Kaufman).

Claim 2 depends on the amended claim 1 and has been amended by introducing additional limitations namely "interrogating the user for access information to the plurality of ISP networks". As amended, claim2 provides the user with the capability of switching between destination ISPs or corporations via the DSM method.

Claim 5 depends on the amended claim 2 and has been amended by introducing additional limitations to better define the invention.

In contrast, (Kaufman) (col. 3, lines 26-40) teaches a method for encrypting access information to access an external network. It doesn't teach the DMS method of the present invention for encrypting the access information for accessing numerous ISP networks.

Accordingly, the encryption method of (Kaufman) could be one of the encryption techniques that may be employed by the DSM method of the present invention for encrypting access information to the numerous ISP networks.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Kaufman) has been traversed.

With regard to Section 14 of the Action, the Examiner has rejected claims 8, 9 & 24 under 35 U.S.C. 103(a) as being unpatentable over (Fuh) in view of "AAA PROTOCOLS: Authentication, Authorization and Accounting for the Internet" (Metz).

(Metz) (p.76, RADIS) and (Fuh) (col.10, lines 49-58) teach that RADIUS and AAA protocol are well known techniques for authenticating user data unit and the applicant agrees with the Examiner on this point.

However, the DSM method, in the present invention, employs standard authentication protocols selected from the list consisting of remote authentication dial-in user service protocol (RADIUS), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), and terminal access controller access control system protocol (TACACS) at the access control node for authenticating users access to the plurality of ISP networks and hence, enabling user networks and users to select from a number of ISPs employing the RADIUS and the AAA protocols for authenticating the user data unit.

Claim 8 depends on the amended claim 1 and has been amended by introducing additional limitations to better define the invention.

Claim 9 depends on the amended claim 1.

Claim 24 depends on the amended claim 15 and has been amended by introducing additional limitations to better define the invention.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Metz) has been traversed.

With regard to Section 15 of the Action, the Examiner has rejected claim 10 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 3 above, in further view of U.S. Patent 5,546,387 to Larsson et al. (Larsson).

The technique for providing the data packet with labels is well known in the art as presented in (Larsson) (col.1, lines 16-27). While the focus in (Larsson) is on labeling of packets, the DSM method, of the present invention, focuses on the ability of user networks and users to select and connect to numerous ISP networks and services, wherein the apparatus for the DSM method employs well-known techniques for labeling packets.

(Larsson) doesn't teach the ability for packet labeling in an apparatus that communicate with numerous ISP networks and services.

Claim 10 depends on the amended claim 3 and 1.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Larsson) has been traversed.

With regard to Section 16 of the Action, the Examiner has rejected claim 14 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 1 above, in further view of U.S. Patent 6,377,955 to Hartmann et al. (Hartmann).

Collecting statistical usage information and data at the access node (col. 1, lines 34-56) for billing and managing an ISP network is well known in the art and the applicant agrees with the Examiner on this point.

However, in the present invention, the access control node in the amended claim 1 collects the statistical usage information for accessing and communicating with the plurality of ISP networks. Accordingly, (Fuh) and (Hartmann) combined don't teach the DSM method of the amended claim 1.

Claim 14 depends on the amended claim 1.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Hartmann) has been traversed.

With regard to Section 17 of the Action, the Examiner has rejected claim 16 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 15 above, in further view of U.S. Patent 5,903,564 to Ganmukhi et al. (Ganmukhi).

Claim 15 is a system claim and has a scope similar to the amended claim 1 and has been amended by introducing additional limitations to better define the invention and to further differentiate from the cited prior art references.

Claim 15 as amended provides an integrated access device (IAD), for placement between a user network and plurality of ISP networks. The IAD comprises a user network interface operatively connecting to plurality of user networks to receive data units from the plurality of user networks. The IAD comprises an authentication agent operatively connected to the user network interface for locally authenticating, authorizing, and forwarding data units received from the plurality of user networks. It also comprises an external network interface operatively connected to the authentication agent for forwarding data units locally authorized by the authentication agent to at least one of the plurality of ISP networks. The IAD comprises means for communicating with the plurality of ISP networks.

The IAD, in the amended claim 15, is designed to connect to numerous network services (ISP networks), whereas in the prior art, systems access devices were designed for communication with specific networks. The IAD is able to interface with and act as an authentication agent for numerous networks and services, thus allowing the user network to connect to any of the supported ISP networks. The IAD interfaces

comprise ingress and egress cards for communicating with the plurality with ISP networks. The ingress and egress cards are well known interface requirements as stated in (Ganmuki) (col. 1, lines 13-29) (that is, switching interfaces for receiving and sending packets that comprise ingress and engross cards).

Claim 16 depends on the amended claim 15.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Ganmuki) has been traversed.

With regard to Section 18 of the Action, the Examiner has rejected claim 18 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 15 above, in further view of U.S. Patent 6,311,275 to Jin et al. (Jin).

As discussed above, claim 15 as amended provides an integrated access device (IAD), for placement between user networks and plurality of ISP networks. The IAD is designed to connect to numerous network services (ISP networks), whereas in the prior art, systems access devices were designed for communication with specific networks. The IAD is able to interface with and act as an authentication agent for numerous networks, thus allowing the user network to connect to any of the supported ISP networks. The IAD authentication agent employs numerous standard protocols and techniques for providing the ability to the user networks (or users) to select and communicate with multiple ISP networks.

In contrast, (Jin) (col. 2, lines 34-44) teaches the protocol for a user communicating with a single network.

Claim 18 depends on the amended claim 15.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Jin) has been traversed.

With regard to Section 19 of the Action, the Examiner has rejected claim 19 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 15 above, in further view of U.S. Patent 6,466,977 to Sitaraman et al. (Sitaraman), (Hartmann), and U.S. Patent 6,510,454 to Walukiewicz (Walukiewicz).

As before, the amended claim 15 provides an integrated access device (IAD), for placement between user networks and plurality of ISP networks. The IAD is designed to connect to numerous network services (ISP networks), whereas in the prior art, systems access devices were designed for communication with specific networks. The IAD is able to interface with and act as an authentication agent for numerous

networks, thus allowing the user network to connect to any of the supported networks. The IAD employs well-known operations and management means for managing the communications between the user networks and the ISP networks. These means include service level enforcing, network resource management, collection of statistical data, and alarm monitoring techniques.

In contrast, (Sitaraman) (col. 3, lines 14-41) teaches the SLA (service level agreement) and AAA services and doesn't teach the management of multiple SLAs and AAA for the numerous ISP networks. Similar arguments for (Hartmann) (col. 1, lines 34-56) and (Walukiewicz) (col. 1, lines 19-33).

Accordingly, (Sitaraman), (Hartmann), and (Walukiewicz) combined do not teach the IAD in the amended claim 15.

Claim 19 depends on the amended claim 15.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Sitaraman), (Hartmann), and (Walukiewicz) has been traversed.

With regard to Section 20 of the Action, the Examiner has rejected claims 21-22 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 15 above, in further view of "PPP Authentication Protocols" by Lloyd et al (Lloyed).

(Lloyd) (pages 1-8, Section 2-3) teaches PAP and CHAP for PPP authentication protocols and doesn't teach the IAD in the amended claim 15.

As before, the IAD, in the amended claim 15, is designed to connect to numerous network services (ISP networks) and hence employs standard authentications and protocols techniques required for communicating with multiple ISP networks and ensuring integrity of the communications between the user and the ISPs. The prior art systems access devices were designed for communication with specific networks. The IAD is able to interface with and act as an authentication agent for numerous networks, thus allowing the user network to connect to any of the supported ISP networks and services.

Claims 21-22 depend on the amended claim 15 and have been amended by introducing additional limitations to better define the invention.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Lloyed) has been traversed.

With regard to Section 21 of the Action, the Examiner has rejected claim 23 under 35 U.S.C. 103(a) as being unpatentable over (Fuh), as applied to claim 15

above, in further view of "An Access Control Protocol, Sometimes Called TACACS" by Finseth (Finseth).

(Finseth) (Page 1, Section 2-3) teaches the terminal access controller access control system and doesn't teach the IAD in the amended claim 15.

As before, the IAD in the amended claim 15 is designed to connect to numerous network services (ISP networks) and hence employs the standard authentication techniques such as TACACS for communicating with the multiple ISP networks, thus allowing the user network to connect to any of the supported ISP networks and services.

Claim 23 depends on the amended claim 15.

It is respectfully submitted that the obviousness rejection of the Examiner in view of (Fuh) and in further view of (Finseth) has been traversed.

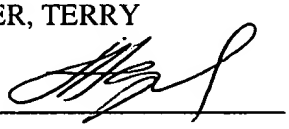
The Examiner is requested to respectfully reconsider this application with regard to the amendments to the claims presented above and the above arguments with a view to considering the claims favorably for allowance.

An **Advisory Action** for this application is respectfully requested at the Examiner's earliest convenience.

The Commissioner is hereby authorized to deduct any prescribed fees for these amendments from our Company's **Deposit Account No. 501832**.

Yours truly,

SKEMER, TERRY

By: 

Victoria Donnelly, Ph.D.
Patent Agent
Reg. No. 44,185

TROPIC NETWORKS INC.,
Intellectual Property Department
135 Michael Cowpland Drive
Kanata, Ontario, Canada K2M 2E9

Telephone: (613) 270-6026
FAX: (613) 270-9663
E-mail: Victoria.Donnelly@tropicnetworks.com

May 30, 2005

CERTIFICATE OF MAILING

I hereby certify that this paper (20 pages) is being sent by FEDEX Courier service in a package having a tracking No. 7929 3554 7700 to the following address:

U.S. Patent and Trademark Office
220 20th Street South
Customer Window,
Mail Stop: Non-Fee Amendment
Crystal Plaza Two, Lobby, Room 1B03
Arlington, VA 22202

Telephone: 703-308-0906

Victoria Donnelly
Director of Intellectual Property
TROPIC NETWORKS INC.,
Intellectual Property Department
135 Michael Cowpland Drive
Kanata, Ontario, Canada.
K2M 2E9

Telephone: (613) 270-6026
FAX: (613) 270-9663
E-mail: vdonnelly@tropicnetworks.com

AMENDMENTS TO THE CLAIMS

WHAT IS CLAIMED IS:

1. (currently amended) A distributed subscriber management method for controlling user authentication at an access control node located between a plurality of user networks and an access network, the access network being connected to ~~an external network having an access rights authentication server~~ plurality of ISP (Internet service Provider) networks, the method comprising the steps of:

(a) receiving, at the access control node, which is operatively connected to the plurality of user networks, a data unit from a user located on one of the plurality of user networks for accessing at least one of the plurality of ISP networks connected to the access network;

(b) determining whether the data unit requires authentication for accessing said at least one of the plurality of ISP networks;

(c) if the data unit requires authentication, determining whether authentication data for said at least one of the plurality of ISP networks is locally stored in a local authorization table on the access control node,

(d) if the authentication data is locally stored in the local authorization table on the access control node, authenticating the data unit, thus preventing unnecessary traffic interchange between the access network, the plurality of ISP networks, and the plurality of user networks;

(e) if the authentication data is not locally stored in the local authorization table on the access control node, determining whether the data unit is eligible for transmission to said at least one of the plurality of ISP networks ~~the external network~~; and

(f) if the data unit is eligible for transmission, transmitting said data unit from the access control node to ~~the authentication server of~~ said at least one of the plurality of ISP networks ~~the external network~~.

2. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (d) includes interrogating the user for access information to the plurality of ISP networks.

3. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (f) comprises ~~a step of~~ receiving, at the access control node, an authentication message for said data unit from the ~~authentication server~~ at least one of the plurality of ISP networks to permit the user to access ~~the external network~~ said ISP network.

4. (canceled) ~~The distributed subscriber management method as claimed in claim 1, wherein the step (b) comprises a step of searching the authenticated data unit locally stored on the access control node~~.

5. (currently amended) The distributed subscriber management method as claimed in claim 2, further including encrypting the access information at the access control node prior to transmitting the access information to ~~the authentication server of the external network~~said at least one of the plurality of ISP networks.

6. (currently amended) The distributed subscriber management method as claimed in claim 3, wherein the step of receiving, at the access control node, the authentication message for said data unit comprises ~~a step of~~ storing authenticated data unit in ~~a~~ the local authorization table on the access control node; and wherein the local authorization table comprises the authenticated data for the plurality of ISP networks.

7. (original) The distributed subscriber management method as claimed in claim 6, wherein the step (b) comprises searching the authenticated data units stored in the local authorization table on the access control node.

8. (currently amended) The distributed subscriber management method as claimed in claim 3, wherein the step (f) comprises ~~a step of~~ communicating with the ~~authentication server~~plurality of ISP networks by employing one or more of standard authentication protocols selected from the list consisting of remote authentication dial-in user service protocol, password authentication protocol, challenge handshake authentication protocol, and terminal access controller access control system protocol.

9. (original) The distributed subscriber management method as claimed in claim 1, wherein the step (d) comprises employing one or more of standard authentication protocols selected from the list consisting of remote authentication dial-in user service protocol, password authentication protocol, challenge handshake authentication protocol, and terminal access controller access control system protocol at the access control node.

10. (original) The distributed subscriber management method as claimed in claim 3, wherein the step (f) further includes packet-labeling of the data unit.

11. (original) The distributed subscriber management method as claimed in claim 6, wherein the step of receiving the authentication message further includes determining the contents of the authentication message at the access control node.

12. (original) The distributed subscriber management method as claimed in claim 1, wherein the step (e) comprises examining the content of the authenticated data unit at the access control node.

14. (original) The distributed subscriber management method as claimed in claim 1, further including collecting statistical usage information at the access node.

15. (currently amended) An integrated access device, for placement between a user network and ~~an external network, the external network having an access rights authentication server~~ plurality of ISP networks, the integrated access device comprising:

(i) a user network interface for operatively connecting to ~~a~~ plurality of user networks to receive data units from the plurality of user networks;

(ii) an authentication agent, operatively connected to the user network interface for locally authenticating, authorizing, and forwarding data units received from the plurality of user networks;

(iii) an external network interface, operatively connected to the authentication agent, for forwarding data units locally authorized by the authentication agent to ~~the external network~~ at least one of the plurality of ISP networks; and

(iv) means for communicating with ~~the~~ said ~~access rights authentication server of the external network~~ plurality of ISP networks.

16. (original) An integrated access device as claimed in claim 15, wherein the user network interface includes a plurality of ingress cards and the external network interface includes an egress card.

17. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a local authorization table for authorizing data units for said plurality of ISP networks.

18. (original) An integrated access device as claimed in claim 15, wherein the authentication agent includes network address assignment and release means.

19. (original) An integrated access device as claimed in claim 15, further including service level enforcing means, network resource management means, means for statistical usage collection, and alarm monitoring means.

20. (currently amended) An integrated access device as claimed in claim 17, wherein the means for communicating with the ~~access rights authentication server~~ plurality of ISP networks comprises:

(p) means for determining whether the data unit is eligible for transmission from the access control node to ~~the authentication server of the external network~~ at least one of the plurality of ISP networks;

(q) means for transmitting the data unit from the access control node to the ~~authentication server of the external network~~plurality of ISP networks;

(r) means for receiving, at the access control node, an authentication message for said data unit from ~~the authentication server~~at least one of said plurality of ISP networks to permit the user to access ~~the external network~~said ISP network; and

(s) means for storing authenticated data units for said plurality of ISP networks in a local authorization table on the access control node.

21. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent ~~includes~~ employs a password authentication protocol.

22. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent ~~includes~~ employs a challenge handshake authentication protocol.

23. (original) An integrated access device as claimed in claim 15, wherein the authentication agent includes a terminal access controller access control system.

24. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent ~~includes~~ employs a remote authentication dial-in user service protocol.

25. (currently amended) An access control node, for placement between ~~a~~ plurality of user networks and ~~an access network, the access network being connected to an external network having an access rights authentication server~~plurality of ISP networks, the access control node comprises the integrated access device claimed in claim 15.